|  |
| --- |
| 3GPP TR 33.881 V0.3.0 (2021-10) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on non-seamless WLAN Offload in 5GS using 3GPP credentials;(Release 17) |
|   |
| *5G-logo_175px* | 3GPP-logo_web |
|  |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. |

|  |
| --- |
|  |
| ***3GPP***Postal address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://www.3gpp.org |
| ***Copyright Notification***No part may be reproduced except as authorized by written permission.The copyright and the foregoing restriction extend to reproduction in all media.© 2021, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).All rights reserved.UMTS™ is a Trade Mark of ETSI registered for the benefit of its members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 4

Introduction 5

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 6

3.3 Abbreviations 7

4 Architectural and security assumptions 7

5 Key issues 7

5.1 Key Issue #1: Support of EAP-AKA’ authentication for NSWO 7

5.1.1 Key issue details 7

5.1.2 Security threats 7

5.1.3 Potential security requirements 7

6 Solutions 8

6.1 Solution #1: Non-Seamless WLAN offload Authentication in 5GS 8

6.1.1 Introduction 8

6.1.2 Solution details 8

6.1.2.1 Architectural overview 8

6.1.2.2 NSWO authentication procedure 9

6.1.3 System impact 11

6.1.4 Evaluation 11

6.2 Solution #2: NSWO authentication using credentials retrieved from UDM/ARPF 12

6.2.1 Introduction 12

6.2.2 Solution Details 12

6.2.2.1 Architecture Overview 12

6.2.2.2 Flows 13

6.2.2.3 Subscriber Privacy 14

6.2.2.4 Key derivation 14

6.2.3 System impact 15

6.2.4 Evaluation 15

6.3 Solution #3: NSWO authentication using credentials retrieved from UDM/ARPF via HSS 16

6.3.1 Introduction 16

6.3.2 Solution Details 16

6.3.2.1 Architecture Overview 16

6.3.2.2 Flows 17

6.3.2.3 SUPI Privacy 19

6.3.2.4 Key derivation 19

6.3.3 System impact 19

6.3.4 Evaluation 20

6.Y Solution #Y: <Solution Name> 21

6.Y.1 Introduction 21

6.Y.2 Solution details 21

6.Y.3 Evaluation 21

7 Conclusions 21

7.1.1 Conclusion for key issue #1 21

Annex A (informative): Change history 22

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# Introduction

Editor’s Note: The text in this clause is not agreed, needs further alignment with feature description and background.

This document aims to study the security procedures necessary to support NSWO in 5GS maintaining security and privacy of users and 5GS network nodes.

In 4G, specifications allow Non-seamless WLAN Offload (NSWO), i.e. allow a UE to connect to a WLAN access network using SIM based access authentication via the mobile network core (as specified in TS 23.402 and in TS 33.402) and to offload selected traffic to the WLAN. This is a deployed feature in 4G networks and enables 4G UEs to connect e.g. to a Wi-Fi venue like a hotel or stadium using SIM based access authentication. This allows the use of mobile network subscription and roaming agreements for WLAN access and for offloading selected traffic to the WLAN where the selection of the traffic to offload is based on policies and where the offloaded traffic is not using 3GPP defined entities. The same feature support is missing so far in 5GS. This Rel-17 study tries to address this gap.

# 1 Scope

The scope of this study is to support Non-seamless WLAN Offload (NSWO) in 5GS. The following will be studied in this SID:

1. Solutions to support NSWO in 5GS
2. Procedures to support authentication methods for the respective solutions in objective.
3. Maintain privacy of subscription identifier similar to 3GPP/non-3GPP access to 5GC, even for NSWO authentication from WLAN.

SA2 positive feedback regarding the architectures for the selected solutions is required before they can proceed to normative phase.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 33.501: “Security architecture and procedures for 5G System”.

[3] 3GPP TS 23.003: "Technical Specification Group Core Network and Terminals; Numbering, addressing and identification".

[4] 3GPP TS 33.402: "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses".…

[5] IETF RFC 5448: " Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')".

[x] <doctype> <#>[ ([up to and including]{yyyy[-mm]|V<a[.b[.c]]>}[onwards])]: "<Title>".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**example:** text used to clarify abstract rules by applying them literally.

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol> <Explanation>

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

<ABBREVIATION> <Expansion>

# 4 Architectural and security assumptions

Editor's note: This clause includes the architectural and security assumptions applicable for the study.

# 5 Key issues

Editor’s Note: This clause contains all the key issues identified during the study.

## 5.1 Key Issue #1: Support of EAP-AKA’ authentication for NSWO

## 5.1.1 Key issue details

For 5G access authentication, two authentication methods EAP-AKA’ and 5G AKA are supported over both 3GPP access and non-3GPP access. Currently the procedure in 3GPP TS 33.402 which are used for (4G) Non-Seamless WLAN Offload (NSWO) over trusted non-3GPP access in 23.402 foresees that the UE may send its IMSI in clear text, i.e. unencrypted, over that air interface and to the AAA server in the core network. To support NSWO for users with credentials defined in a 5GC, the NSWO authentication procedure needs to make use of credentials provided by the 5GC (i.e. by the UDM/ARPF in the 5GC). The new NSWO authentication procedures should also support the same or similar level of security and privacy as in 5GS, i.e. to never expose the IMSI/SUPI in the clear. Since the UEs may be provisioned by the operators to use EAP-AKA’, this may be the easiest authentication method to be adopted for 5G NSWO.

Currently installed WLAN APs support only EAP authentication framework over Radius or Diameter interface to an operator owned AAA. Since the 5GC is able to support a unified authentication method, including EAP-AKA’ the same could be extended to support NSWO using the same credentials.

Reusing the same EAP-AKA’ infrastructure for the NSWO authentication can provide 5G equivalent authentication security to enterprise users as well.

### 5.1.2 Security threats

UEs need to be authenticated when they are connected to WLAN APs for availing NSWO, otherwise the NSWO could be misused by fraudulent UEs. Fraudulent UEs accessing enterprise WLAN without authentication can consume the WLAN resources and prevent the NSWO for legitimate UEs. This can cause DDoS scenarios for NSWO UEs.

If subscriber identity privacy is not available during authentication procedure, then tracking of the subscriber with “IMSI catchers” can lead to trackability and linkablity attacks.

### 5.1.3 Potential security requirements

The 5GS shall support EAP-AKA’ authentication method using 5GC credentials for NSWO.

# 6 Solutions

## 6.1 Solution #1: Non-Seamless WLAN offload Authentication in 5GS

### 6.1.1 Introduction

This solution addresses key issue #1 Support of EAP-AKA’ authentication for NSWO.

### 6.1.2 Solution details

#### 6.1.2.1 Architectural overview

The authentication procedure is modelled after the existing EAP-AKA' authentication procedure in 5GS. A new network function NSWO NF is introduced to support NSWO authentication procedure and isolate AUSF from direct access by the external WLAN infrastructure. NSWO NF is connected to non-3GPP access WLAN AP via SWa interface (could be over RADIUS or Diameter interface) allowing to keep the Wi-Fi (authentication related) infrastructure unchanged. The NSWO NF is connected via a new interface, Nx, to the AUSF (thus avoiding a direct connection from WLAN to AUSF).



**Figure 6.1.2.1-1: NSWO NF between 5GS and WLAN AP**



**Figure 6.1.2.1-2: NSWO Architecture proposal**

#### 6.1.2.2 NSWO authentication procedure

 

 **Figure 6.1.2.2-1: NSWO Authentication procedure**

1. If the HPLMN supports 5G NWSO and wants the UE to use it for NSWO, then the HPLMN configures the UE to always use 5G NSWO. This configuration can be either on the USIM or ME, with configuration on the USIM taking precedence over the ME.
2. A connection is established between the UE and the WLAN AP, using a specific procedure based on IEEE 802.11.
3. The WLAN AP sends an EAP Identity Request to the UE.
4. The UE always send the SUCI in NAI format (i.e., username@realm format) irrespective of whether SUPI Type configured on the USIM is IMSI or NAI.

Editor’s Note: username@realm format will need to be specified for SUCI in NAI format in clause 28.7.3 of TS 23.003.

1. The WLAN AP sends a SWa protocol message (could be over RADIUS or Diameter interface) with EAP identity response, NAI containing the SUCI to new entity NSWO network function (NSWO NF).

NOTE 1: NSWO NF acts as SBI/AAA proxy between the AUSF and the WLAN Access Point.

1. The NSWO NF sends the message Nausf\_UEAuthentication\_Authenticate Request with SUCI, Serving network name and NSWO indicator towards the AUSF. NSWO\_indicator conveys the information to the AUSF that this authentication procedure is triggered for Non-seamless WLAN offload purposes.

NOTE 2: Serving Network Name used between UE and HN could be pre-agreed default SN Name (for example 5G:NSWO) or pre-configured WLAN ID for NSWO purpose only.

1. The AUSF (EAP authentication server) sends a Nudm\_UEAuthentication\_Get Request to the UDM including SUCI and NSWO indicator.

NOTE 3 Whether existing service operations used for primary authentication (Nausf\_UEAuthentication\_Authenticate and Nudm\_UEAuthentication\_Get) can be resused for NSWO or new service operations for NSWO execution independent from primary authentication service operations (e.g., Nausf\_UEAuthentication\_NSWOAuthenticate and Nudm\_UEAuthentication\_GetNSWO) are to be defined, will be decided in the normative phase.

1. Upon reception of the Nudm\_UEAuthentication\_Get Request, the UDM invokes SIDF if a SUCI is received. SIDF de-conceal SUCI to gain SUPI before UDM can process the request. UDM generates the EAP-AKA’ authentication vector (RAND, AUTN, XRES, CK´ and IK´) based on SN name or NSWO indication and passes it along with SUPI to AUSF in a Nudm\_UEAuthentication\_Get Response message.
2. The AUSF stores XRES for future verification. The AUSF sends the EAP-Request/AKA'-Challenge message to the NSWO NF in a Nausf\_UEAuthentication\_Authenticate Response message.
3. The NSWO NF sends SWa protocol message with EAP-Request/AKA'-Challenge message to the WLAN AP.
4. The WLAN AP forwards the same EAP-Request/AKA'-Challenge message to the UE.
5. At receipt of the RAND and AUTN, the ME construct the SN name, and the USIM in the UE verifies the freshness of the AV' by checking whether AUTN can be accepted as described in TS 33.102. If so, the USIM computes a response RES. The USIM returns RES, CK, IK to the ME. The ME derives CK' and IK' according to TS 33.501[2] Annex A.3. If the verification of the AUTN fails on the USIM, then the USIM and ME proceed as described in TS 33.501[2] sub-clause 6.1.3.3. The UE derives the MSK and EMSK as described in RFC 5448[5]. The UE may use MSK as the pre-shared key for 4-way handshake when it is using NSWO. When the UE is using NSWO, the KAUSF is not needed to be generated by the UE.
6. The UE sends the EAP-Response/AKA'-Challenge message to the WLAN AP.
7. The WLAN AP forwards the EAP-Response/AKA'-Challenge message in SWa protocol message to NSWO NF.
8. The NSWO NF sends the Nausf\_UEAuthentication\_Authenticate Request with EAP-Response/AKA'-Challenge message to AUSF.
9. The AUSF verifies if the received response RES matches the stored and expected response XRES. If the AUSF has successfully verified, it will continue as follows to step 16, otherwise it will return an error to the NSWO NF. The AUSF does not trigger linking increased home control to subsequent procedures.
10. The AUSF derives the required MSK key from CK’ and IK’ as per Annex F of TS 33.501 and EMSK as described in RFC 5448[5]. The AUSF sends Nausf\_UEAuthentication\_Authenticate Response message with EAP-success, MSK key to NSWO NF.

NOTE 4: AUSF could also optionally provide SUPI to NSWO NF.

1. When the AUSF performs the NSWO authentication, the KAUSF is not needed to be generated by the AUSF.
2. The NSWO NF sends a SWa protocol message with EAP-success and MSK to WLAN. EAP-success message is forwarded from WLAN AP to the UE. The master key (MSK) is passed on by the NSWO NF to WLAN AP.

 Further WLAN keys may be generated in UE and WLAN AP independently. When a 4-way handshake is executed (see IEEE 802.11) which establishes a security context between the WLAN AP and the UE.

### 6.1.3 System impact

NSWO NF:

- New NF which needs to support enhanced Diameter SWa protocol to access points and SBI towards AUSF for authentication.

AUSF:

- Modifications to primary authentication Nausf\_UEAuthentication\_Authenticate, modifications to AUSF logic for primary authentication, modification to key hierarchy handling

UDM

-

UE:

- Support for SUCI for 5G NSWO.

### 6.1.4 Evaluation

The existing AAA server can be modified with the new NSWO NF functionality.

Existing EAP-AKA’ authentication is adapted with impact on network nodes and UE and fulfiling to the NSWO requirement.

The solution proposes to reuse existing AUSF/UDM services of primary authentication for 5G NSWO. It would impact on primary authentication architecture, procedures and key hierarchy handling:

- Technically it is feasible to use AUSF as EAP server and UDM for AV generation and SUPI Privacy for 5G NSWO. But it requires yet different logic in AUSF, e.g., to handle NSWO authentication different from primary authentication and different key hierarchy handling based on different input.

- Assumed that a subset of SWa is required and a new reference point might be needed.

## 6.2 Solution #2: NSWO authentication using credentials retrieved from UDM/ARPF

### 6.2.1 Introduction

This solution addresses key issue #1 (Support of EAP-AKA’ authentication for NSWO). This solution corresponds to a scenario where NSWO is executed for a user defined in a 5GC and the 5GC does not support interworking with EPC. This is, the home network of the user does not support HSS functionality. The solution also covers the case when the 5G user makes use of a 4G ME and the case of a 5G user using pre-Rel-17 5G ME which does not support 5G NSWO of Rel-17.

### 6.2.2 Solution Details

### 6.2.2.1 Architecture Overview

The architecture proposed by this solution is similar to the existing one in EPC. The 3GPP AAA server fetches authentication vectors over Diameter interface SWx. However, since HSS is not present it is proposed that an AAA-IWF is deployed to relay authentication vectors requests and perform related protocol conversion between Diameter SWx and SBA services towards the UDM/ARPF in the 5GC. The AAA-IWF can be realized by the NSSAAF and use existing N59 reference point with the UDM/ARPF.

Additionally, this solution can also support SUPI privacy. This requires the 3GPP AAA to use updated SWx or new diameter interface, called SWx’ here, that includes the SUCI instead of an IMSI as UE ID.

The assumed architecture is described in Figure 6.2.2.1-1.



Figure 6.2.2.1‑1: NSWO access authentication using credentials retrieved from UDM/ARPF

### 6.2.2.2 Flows

Figure 6.2.1.2‑1: Non-3GPP access authentication in 5GC via UDM

0. The UE selects a WLAN access network and a PLMN for performing 3GPP based access authentication via this PLMN.

1. A layer-2 connection is established between the UE and the WLAN access network.

2. The EAP authenticator in the WLAN access network sends an EAP Request/Identity to the UE.

3. The UE sends an EAP Response/Identity message. The UE shall send its identity complying with Network Access Identifier (NAI) format specified in TS 23.003 [3]. In case of a 5G ME, the NAI contains either a pseudonym allocated to the UE in a previous run of the authentication procedure or, in the case of first authentication, the SUCI. In case of a 4G ME, the NAI contains either a pseudonym allocated to the UE in a previous run of the authentication procedure or, in the case of first authentication, the IMSI.

4. The message is routed towards the proper 3GPP AAA Server based on the realm part of the NAI as specified in TS 33.402 [4]. The routing path may include one or several AAA proxies. In such cases, NAI is formed in decorated NAI format as specified in TS 23.003 [3].

5. When the 3GPP AAA Server receives the EAP Response/Identity message that contains the subscriber identity that is SUCI in NAI format, the 3GPP AAA decides to fetch SUPI(containing IMSI or taking the form of NAI) and authentication vectors from the UDM/ARPF via SWx'.

In case the NAI received from step 4 does not contain a SUCI (i.e., the 5G user accesses the WLAN access network with a 4G ME or 5G user using pre-Rel-17 5G ME which does not support 5G NSWO of Rel-17 and provides an IMSI), the 3GPP AAA server gets IMSI from NAI and request authentication vectors using the existing SWx diameter MAR command.

Similarly, in case the NAI received from step 4 contains a SUCI protected with Null scheme, the 3GPP AAA server may retrieve the SUPI from the SUCI and request authentication vectors using the existing SWx diameter MAR command.

6. The 3GPP AAA Server sends an Auth Vector request with SUCI or IMSI, and the access network identity received from step 4. The request is routed via an AAA-IWF/NSSAAF over SWx/SWx' and sent towards the UDM/ARPF of the 5GC via the AAA-IWF/NSSAAF. In the case that the SUCI is included in the request, this message could be an enhancement to SWx messages, e.g. Multimedia-Auth-Request/ Multimedia-Auth-Answer, as specified in TS 33.402 [4]. Otherwise, if IMSI can be used, the existing diameter SWx MAR commands could be used as defined.

7. The AAA-IWF/NSSAAF discovers and selects an UDM e.g. based on the routing identifier of the SUCI and sends an Auth Vector Request, e.g., via a new Nudm\_UEAuthentication\_GetAaaAV service operation, with the SUCI or SUPI, the access network identity and an indication for the requesting node is 3GPP AAA server.

NOTE 1: If AAA-IWF/NSSAAF receives IMSI from step 6, the AAA-IWF/NSSAAF derives SUPI from the IMSI.

8. If SUCI was received, the UDM de-conceals the SUPI from the SUCI. The UDM selects EAP-AKA' as authentication method, e.g. based on UE's subscription, the access network identity and an indication for the requesting node is 3GPP AAA server. The UDM/ARPF generates the AKA AV of EAP-AKA’.

9. The UDM sends the Auth Vector Response to the AAA-IWF/NSSAAF with the selected authentication method, AKA AV and SUPI if SUCI is received in step7.

10. The AAA-IWF/NSSAAF sends the Auth Vector Response to the 3GPP AAA server over SWx/SWx' with the selected authentication method, AKA AV and SUPI.

11. The 3GPP AAA server and the UE proceed with EAP AKA' procedure and derive key materials e.g. MSK/EMSK as specified in TS 33.402 [4].

12. The 3GPP AAA Server sends the EAP Success message and the MSK to the authenticator in the WLAN access network.

13. The authenticator in the WLAN access network informs the UE about the successful authentication with the EAP Success message.

14. The UE and the WLAN access network proceed with security establishment based on the share keying material. After successful authentication, the UE receives its IP configuration from the WLAN access network and can exchange IP data traffic directly via the WLAN, i.e. using NSWO.

### 6.2.2.3 Subscriber Privacy

The UE determines whether 5G subscriber privacy should be used for NSWO traffic, based on the local configuration or the information provisioned by the home network that the home network supports 5G privacy for access authentication for NSWO.

NOTE: Depending on ME or USIM capability and UE's subscription, there could be cases that a 5G user can't apply SUCI for NSWO, e.g., the UE has 5G subscription defined in the home network but the terminal is pre-R15.

The UE follows the subscriber privacy for EAP-AKA' as specified in TS 33.501 [2] Annex F. In addition, the UE supports pseudonym NAI that are allocated to the UE by the 3GPP AAA server in a previous run of the authentication procedure, in response to EAP-Request/Identity or EAP-Request/AKA-Identity messages.

When the UE determines 5G subscriber privacy is not applicable for NSWO, the UE uses the NAIs specified in EPC for non-3GPP access interworking as in TS 33.402 [4].

### 6.2.2.4 Key derivation

When deriving CK' and IK' then the KDF of TS 33.402 [11] clause A.2 is used.

When deriving MSK/EMSK for EAP-AKA' ( i.e. MK = PRF'(IK'|CK',"EAP-AKA'"|Identity)), the UE and the 3GPP AAA follows the Identity used for key derivation as specified in TS 33.501 [2] Annex F, in case the UE determines 5G subscriber privacy is applicable for NSWO, i.e. SUCI is used in NSWO access authentication.

### 6.2.3 System impact

The solution has the following impacts on the different functions:

Untrusted non-3GPP access: None

UE:

- Supports SUCI as EAP identity for NSWO authentication procedure

- Supports indication provisioned from the home Network whether 5G privacy is supported for NSWO.

3GPP AAA server:

- Support SUCI for access authentication for 5G NSWO. Optionally, extract SUPI from SUCI protected with Null scheme.

- Support Diameter SWx' to retrieve SUPI (containing IMSI or taking the form of NAI) and AV.

- Support Key derivation (MSK/ESMK) based on 5G EAP-AKA' profile

AAA-IWF/NSSAAF:

- Support protocol conversion between Diameter SWx/SWx' and corresponding SBA service operations with UDM

- New interaction with UDM to retrieve NSWO AV

NOTE: NSSAAF already supports selection of UDM via NRF so this is not considered as an impact.

UDM:

- Support SUCI deconcealment and AV request from 3GPP AAA via AAA-IWF

AUSF: N/A

HSS: None

### 6.2.4 Evaluation

This solution fulfills the requirement of Key Issue #1.

The solution has no impact on underlying access architecture.

- Leverages on existing 4G NSWO infrastructure (i.e., 3GPP AAA remains as EAP Server).

- Supports Coexistence with 4G NSWO deployments and devices/subscriptions.

The solution introduces a new service in UDM to provide AV for 5G NSWO and new procedure in AAA-IWF/NSSAAF to support protocol conversion between Diameter and SBI.

The solution is independent from primary authentication architecture, 5G key hierarchy and registration.

The solution has impacts in 3GPP AAA to support SUPI privacy.

3GPP AAA needs to be supported for NSWO in standalone 5GC deployment.

## 6.3 Solution #3: NSWO authentication using credentials retrieved from UDM/ARPF via HSS

### 6.3.1 Introduction

This solution addresses key issue #1 (Support of EAP-AKA’ authentication for NSWO). This solution corresponds to a scenario where NSWO is executed for a user defined in a 5GC and the 5GC supports interworking with EPC. This is, the home network of the user supports HSS functionality. The user may be a 5G user allowed to interwork with EPC or a 5G only user.

### 6.3.2 Solution Details

### 6.3.2.1 Architecture Overview

The architecture proposed by this solution supports co-existence with EPC. The 3GPP AAA server requests authentication vectors from the HSS over SWx.

If the HSS supports the authentication vector generation function for this user, then the HSS can provide the authentication vectors to the 3GPP AAA server as currently defined.

However, if the authentication vector generation function for this user has been moved to the UDM/ARPF, the HSS requests the authentication vectors from the UDM/ARPF using UDICOM NU1 reference point.

The architecture is described in Figure 6.3.2.1-1.



Figure 6.3.2.1‑1: NSWO access authentication in 5GC via HSS

In scenarios where the Home Network supports a mixture of 4G only users, 5G users supporting interworking with EPC and 5G only users, an SLF/DRA can assist in routing the authentication vector requests towards the HSS (for 4G only users, 5G users supporting interworking with EPC) or towards UDM/ARPF (for 5G only users) via an AAA-IWF realized by the NSSAAF as described in solution 6.2.

This alternative architecture is described in Figure 6.3.2.1-2.



Figure 6.3.2.1‑2: NSWO authentication in 5GC via SLF/DRA

Additionally, this solution can also support SUPI privacy. This requires the 3GPP AAA to use updated SWx or new diameter interface, called SWx’ here, that includes the SUCI instead of an IMSI as UE ID. The SLF/DRA also assists in routing new or updated Diameter SWx’ requests towards the UDM/ARPF via the AAA-IWF/NSSAAF as described in the next section.

### 6.3.2.2 Flows

Figure 6.3.1.2‑1: Non-3GPP Access authentication using credentials retrieved from UDM/ARPF via HSS

Steps 0 to 4 are the same as described for solution 6.2.

NOTE: In case NAI received from step4 does not contain a SUCI (i.e. contains an IMSI), the 3GPP AAA server retrieves IMSI from the NAI and authentication vectors from the HSS via SWx (steps 11b-13b) as in existing EPC procedure.

5. The 3GPP AAA Server receives the EAP Response/Identity message that contains the subscriber identity that is SUCI in NAI format. The 3GPP AAA decides to fetch authentication vectors from the UDM (referring step 6a) or from the HSS (referring step 6b to step 13b) based on local policy.

6a. The 3GPP AAA Server retrieves the authentication vectors from the UDM/ARPF via AAA-IWF with an updated Diameter MAR SWx’ request which includes SUCI and the access network identity received in step 4 in the request message, as defined in solution 6.2. An SLF/DRA assists in routing updated Diameter SWx’ requests towards the UDM/ARPF via the AAA-IWF/NSSAAF. The flows continue with step14.

6b. The 3GPP AAA Server sends an IMSI retrieval request with SUCI received from step 4 via a new Diameter command over SWx’. An SLF/DRA assists in routing the new Diameter SWx’ request towards the UDM/ARPF via the AAA-IWF/NSSAAF.

NOTE: In case NAI received from step4 contains a SUCI protected with Null Scheme, the 3GPP AAA server may retrieve IMSI from the SUCI by itself and skip step 6b to step10b.

7b. The AAA-IWF/NSSAAF discovers and selects an UDM e.g. based on the routing identifier of the SUCI and sends SUCI Deconcealment Request using a new Nudm service, e.g. Nudm\_SUCIDeconcealment\_Get, to the UDM.

8b. The UDM de-conceals the SUPI from the SUCI.

9b. The UDM sends the SUCI Deconcealment Response to the AAA-IWF/NSSAAF with the SUPI.

10b. The AAA-IWF/NSSAAF converts SUPI into IMSI and sends the IMSI retrieval Response to the 3GPP AAA server over SWx'.

11b. The 3GPP AAA Server sends an Auth Vector request with IMSI and the access network identity received from step 4. The request is routed to the HSS via SWx as currently specified. In the presence of multiple HSS instances in the Home Network of the user, an SLF/DRA will assist in routing the SWx request to the HSS where the user is defined.

In scenarios where the Home Network supports a mixture of 4G only users, 5G users supporting interworking with EPC and 5G only users, the SLF/DRA can also assist in routing the authentication vector requests towards the HSS (for 4G only users, 5G users supporting interworking with EPC) or towards UDM/ARPF (for 5G only users) via an AAA-IWF realized by the NSSAAF as described in solution 6.2.

12b. If the HSS supports the authentication vector generation function for this user, then the HSS provides the authentication vectors to the 3GPP AAA server as currently defined. If the authentication vector generation function for this user has been moved to the UDM/ARPF, the HSS requests the authentication vectors from the UDM/ARPF using UDICOM NU1 reference point as currently specified.

13b. The HSS sends the Auth Vector Response to the 3GPP AAA server over Diameter SWx.

Steps 14 to 17 are the same as described for solution 6.2.

### 6.3.2.3 SUPI Privacy

The UE follows the subscriber privacy for EAP-AKA' as specified for solution 6.2.

### 6.3.2.4 Key derivation

Derivation of CK' and IK' and MSK/EMSK for EAP-AKA' are as specified for solution 6.2.

### 6.3.3 System impact

The solution has the following impacts on the different functions:

UE:

- Supports SUCI as EAP identity for 5G NSWO authentication procedure

- Supports indication provisioned from the home Network whether 5G privacy is supported for NSWO.

3GPP AAA server:

- Support SUCI for access authentication for NSWO. Optionally, extract IMSI from SUCI protected with Null scheme. - Support Diameter SWx' to retrieve IMSI

- Support Key derivation (MSK/EMSK) based on 5G EAP-AKA' profile

AAA-IWF/NSSAAF:

- Support protocol conversion between DiameterSWx/ Swx' and SBA interface with UDM

UDM:

- Support SUCI deconcealment request from 3GPP AAA via AAA-IWF/NSSAAF

NOTE: NSSAAF already supports selection of UDM via NRF so this is not considered as an impact.

SLF/DRA:

- Support routing of updated and/or new SWx’ diameter commands.

AUSF: N/A

HSS: None

Untrusted non-3GPP access: None

### 6.3.4 Evaluation

This solution fulfills the requirement of Key Issue #1.

The solution has no impact on underlying access architecture

- Leverages on existing 4G NSWO infrastructure (i.e., 3GPP AAA remains as EAP Server).

- Supports Coexistence with 4G NSWO deployments and devices/subscriptions.

The architecture has already been supported in Rel16 specifications for 4G subscriptions and 5G subscriptions supporting EPS IWK when there is no SUPI privacy required. The solution has impacts in 3GPP AAA to support SUPI privacy.

The solution introduces new service in UDM to provide AV for 5G NSWO and new procedure in AAA-IWF/NSSAAF to support protocol conversion between Diameter and SBI.

The solution is independent from primary authentication architecture, 5G key hierarchy and registration.

This solutions addresses scenarios where the USIM stores an IMSI. All the scenarios where the USIM stores the SUPI in NAI format are not taken into consideration.

## 6.Y Solution #Y: <Solution Name>

### 6.Y.1 Introduction

Editor’s Note: Each solution should list the key issues being addressed.

### 6.Y.2 Solution details

### 6.Y.3 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

# 7 Conclusions

Editor’s Note: This clause contains the agreed conclusions that will form the basis for any normative work.

# 7.1.1 Conclusion for key issue #1

Solution#1 is selected as the basis for the normative work of key issue#1 “Support of EAP-AKA’ authentication for NSWO” with the main charactetistics as follows

- The WLAN access is connected to a new NSWO NF which acts as a proxy of NSWO authentication requests towards the 5GS.

- The UE makes use of a SUCI which is deconcealed by the 5GS in the UDM/SIDF.

NOTE: Aspects related to co-existence with 4G NSWO deployments, support of EPS interworking and support of pre-Rel17 UEs have not been considered for the conclusions output of this TR.

Annex A (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2021-05 | SA3#103-e | S3-211515 |  |  |  | TR Skeleton | 0.0.0 |
| 2021-05 | SA3#103-e | S3-212148, S3-212149, S3-212150 |  |  |  |  | 0.1.0 |
| 2021-08 | SA3#104-e | S3-213037,S3-213091,S3-212875 |  |  |  | New solution added for key issue#1 | 0.2.0 |
| 2021-10 | SA3#104-e Ad-hoc | S3-213590,S3-213349,S3-213670,S3-213451,S3-213712,S3-213350,S3-213545,S3-213711,S3-213351,S3-213548,S3-213591 |  |  |  | Solution and evaluation updates.Conclusion of the key issue#1 | 0.3.0 |